



Billing Code: 4410-02-P

DEPARTMENT OF JUSTICE

[CPCLO Order No. 009-2019]

Privacy Act of 1974; System of Records

AGENCY: Federal Bureau of Investigation, United States Department of Justice.

ACTION: Notice of a Modified System of Records.

SUMMARY: Pursuant to the Privacy Act of 1974 and Office of Management and Budget (OMB) Circular No. A-108, notice is hereby given that the Federal Bureau of Investigation (FBI), a component within the United States Department of Justice (DOJ or Department), proposes to modify an existing system of records notice titled The Next Generation Identification (NGI) System, JUSTICE/FBI-009. The FBI proposes to add iris images as another biometric in NGI, include fingerprints voluntarily submitted to NGI by individuals appealing firearms denials or seeking a review of their NGI identity records, include the testing environments of NGI, and clarify the biographic records in NGI.

DATES: In accordance with 5 U.S.C. 552a(e)(4) and (11), the public has 30 days in which to comment on the routine uses, described below. Please submit any comments by **[INSERT DATE 30 AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: The public, OMB, and Congress are invited to submit any comments by mail to the United States Department of Justice, Office of Privacy and Civil Liberties, ATTN: Privacy Analyst, 145 N St., NE, Suite 8W-300, Washington, DC 20530; by facsimile at 202-307-0693; or by email at privacy.compliance@usdoj.gov. To ensure proper handling, please reference the above CPCLO Order No. on your correspondence.

FOR FURTHER INFORMATION CONTACT: Roxane M. Panarella, Privacy Attorney, Criminal Justice Information Services (CJIS) Division, 1000 Custer Hollow Road, Clarksburg, WV 26306; telephone (202) 324-3000.

SUPPLEMENTARY INFORMATION: The NGI SORN is being republished due to several changes since its last publication in May of 2016. The following updates are being made: (1) The inclusion of iris images as a biometric; (2) the inclusion of individuals who voluntarily provide fingerprints and associated information in order to appeal firearm denials; (3) the inclusion of individuals who voluntarily provide fingerprints and associated information in order to obtain their own identity history records; (4) the inclusion of data in the testing environments of NGI; and (5) the clarification that some identity records contain only biographic information.

Iris images: As described in the previously published NGI SORN, one of the significant changes from the FBI's predecessor system, the Integrated Automated Fingerprint Identification System (IAFIS), was the implementation of NGI's additional biometric services. While IAFIS had been primarily a fingerprint system, NGI now offers the retention and searching of additional biometrics, such as facial images and palm prints. NGI continues to rely on ten-print fingerprints for positive identification but its identity records may contain multi-modal biometrics to augment those fingerprints and associated biographic information. For the past few years, the FBI has conducted a pilot to determine if iris images would be an appropriate and useful addition to the NGI operational environment. The FBI has coordinated with criminal justice and scientific partners to determine the efficacy of using iris images for biometric identification purposes. Based on the pilot findings, the FBI has determined that iris matching is highly accurate; therefore, the addition of iris images in the NGI operational environment would be of great value. The FBI plans to permit authorized users of NGI to enroll and search iris

images in the near future. Although the May 2016 NGI SORN used the terms “biometrics” and “biometric images” which would include iris images, in the interest of clarity, the FBI has decided to specifically add “iris images” to all appropriate categories of individuals and categories of records in this SORN.

Firearms denials: In accordance with the Brady Handgun Violence Prevention Act of 1993, the FBI uses the National Instant Criminal Background Check System (NICS) to conduct background checks on potential buyers of firearms. If the FBI denies the transfer of the firearm based on federal or state prohibiting criteria, the individual has a right, per federal statute, to request the reason for the denial and to appeal that denial. An individual may voluntarily provide fingerprints to the FBI in support of the appeal. The FBI has been conducting NICS background checks for decades; however, with the passage of the Fix NICS Act in 2018, it sought ways to expedite the appeal process. If an individual submits fingerprints, the FBI now conducts electronic searches of the fingerprints and associated biographic information in NGI to locate relevant criminal history. The fingerprints and other personally identifiable information are not retained, and are permanently deleted from NGI, after the search is conducted. The FBI is updating the categories of individuals and categories of records in this SORN to include fingerprints voluntarily submitted to NGI for firearms appeals.

Identity History Records: Pursuant to 28 CFR 16.30-16.34, issued in 1973, an individual may seek a copy of his or her identification record, or the lack thereof, for the purposes of access and amendment. The relevant federal regulations require that an individual provide fingerprints and specific biographic information to the FBI in order to ensure positive identification and accurate record retrieval. The fingerprints and associated personal information are retained in NGI for a period of three years. In addition, 28 CFR 50.12 provides that

individuals have a right to appeal the accuracy of their identification records. For the past several decades, the FBI has processed millions of these requests and appeals. In so doing, the FBI has offered a valuable service to the public, affording individuals the opportunity to review, correct, or update criminal history records or receive confirmation of the absence of criminal history records. The May 2016 SORN included this population within Routine Use X; however, the FBI finds that this population is more appropriately placed within categories of individuals and categories of records. Therefore, the text has been removed from the Routine Uses and the appropriate updates are being made to the other sections of this SORN.

Testing Environments: NGI permits its users to test its various services prior to participation in the NGI operational system. This allows users to prepare for technical changes, system upgrades, and new requirements. NGI has both operational and non-operational testing environments that ensure ongoing data and system security, access, and integrity. The “operational testing environments” use live data to test functions of the NGI system in limited access environments disconnected from the rest of the environments. This data is largely duplicative of the data in the NGI operational system. The “non-operational” testing environments” use simulated data to test functions of the NGI system in limited access environments disconnected from the rest of the environments. Testing data in both operational and non-operational environments consists of the same types of biometric and biographic information contained in the NGI operational system. This SORN adds the NGI testing environments and the data contained within as part of the NGI system.

Biographic Records: Although NGI is primarily a biometric system, in rare instances, the FBI may be unable to obtain fingerprints or other biometrics associated with an individual. This situation may occur with identities collected pursuant to the FBI’s criminal and national

security investigative missions, as well as some limited instances of identities submitted for background checks or clearances. In all instances, the FBI ensures that the biographic information is as accurate, complete, and up-to-date as reasonably possible and seeks to obtain fingerprints for the record. In the interest of transparency, the FBI is clarifying the presence of biographic-only records in this SORN.

In accordance with 5 U.S.C. 552a(r), the Department has provided a report to OMB and Congress on this new system of records.

Dated: September 30, 2019.

Peter A. Winn,

Acting Chief Privacy and Civil Liberties Officer,

United States Department of Justice.

JUSTICE/FBI-009

SYSTEM NAME AND NUMBER:

The Next Generation Identification (NGI) System, JUSTICE/FBI-009.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Records described in this notice are maintained at the Federal Bureau of Investigation (FBI), Criminal Justice Information Services Division (CJIS), Clarksburg, WV. Some or all system information may be duplicated at other locations, including at FBI facilities, for purposes of system backup, emergency preparedness, and continuity of operations. Records may also be maintained in secure cloud computing environments. Cloud computing service providers may change. The cloud computing service provider on the date of this publication is

the Amazon Web Services Commercial Cloud. For information about the current cloud computing service provider, please contact the Unit Chief, Privacy and Civil Liberties Unit, Office of the General Counsel, FBI, 935 Pennsylvania Avenue, NW, Washington, DC 20535-0001; telephone 202-324-3000.

SYSTEM MANAGER(S):

Assistant Director, Criminal Justice Information Services Division, Federal Bureau of Investigation, 1000 Custer Hollow Road, Clarksburg, WV 26306.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Authorities for the maintenance of these records include 28 U.S.C. 534; 34 U.S.C. 41101; 28 CFR 0.85(b)&(j), and Part 20.

PURPOSE(S) OF THE SYSTEM:

The purposes for maintaining the NGI system include identification and criminal history information functions in order to perform non-criminal justice background checks, to enforce criminal laws, to further national security, and to assist with humanitarian efforts. The NGI system maintains and disseminates relevant records to local, state, tribal, federal, foreign, and international criminal justice agencies, as well as non-criminal justice agencies and other entities where authorized by federal statute, state statute pursuant to 34 U.S.C. 41101, Presidential executive order, or regulation of the Attorney General of the United States. In addition, identification assistance is provided in disasters and for other humanitarian purposes.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

- A. Individuals fingerprinted as a result of a criminal inquiry, a lawful detention, an arrest, incarceration, or immigration or other civil law violation;

- B. Individuals fingerprinted for the purposes of employment, licensing, military service, or volunteer service;
- C. Individuals fingerprinted for the purposes of security clearances, suitability determinations, or other background checks;
- D. Individuals fingerprinted for the purposes of immigration benefits, alien registration and naturalization, or other governmental benefits;
- E. Individuals whose fingerprints or biographic information have been obtained pursuant to the FBI's authority to identify and investigate federal crimes and threats to the national security;
- F. Individuals whose fingerprints or other biometrics have been received from foreign countries or international organizations pursuant to sharing agreements;
- G. Individuals whose biometrics (e.g. palm prints, facial images, iris images) have been obtained as a result of a criminal inquiry, a lawful detention, an arrest, incarceration, or immigration or other civil law violation;
- H. Individuals who have provided biometrics (e.g. palm prints, facial images, iris images) for the purposes of employment, licensing, military service, or volunteer service;
- I. Individuals who have provided biometrics (e.g. palm prints, facial images, iris images) for the purposes of security clearances, suitability determinations, or other background checks;
- J. Individuals who have provided biometrics (e.g. palm prints, facial images, iris images) for the purposes of immigration benefits, alien registration and naturalization, or other governmental benefits;

- K. Individuals whose biometrics (e.g. palm prints, facial images, iris images) have been obtained pursuant to the FBI's authority to identify and investigate federal crimes and threats to the national security;
- L. Individuals whose fingerprints or other biometrics have been retrieved from locations, property, or persons associated with criminal or national security investigations;
- M. Missing persons, unidentified persons, or others whose fingerprints or other biometrics have been submitted in support of disaster response, humanitarian efforts, or similar purposes;
- N. Individuals whose fingerprints or other biometrics have been retained at their request or consent for personal identification purposes;
- O. Individuals whose biographic and/or biometric information may be retained due to their official duties associated with the processing of system records (e.g. system administrators, fingerprint collectors) or in their roles as authorized users of the system;
- P. Individuals who have provided fingerprints or biographic and/or supplementary information to request the reason for a firearm transfer denial or delay, appeal/challenge a denial of a firearm transfer, or otherwise inquire about a National Instant Criminal Background Check System transaction;
- Q. Individuals who have provided fingerprints and associated biographic and/or supplementary information to obtain identity history record information for access, amendment, or appeal;
- R. Individuals who have submitted biographic information for the purposes of federal employment, contract employment, security clearances, suitability determinations, or background checks;

- S. Individuals who have provided fingerprints, biometrics, and/or biographic information to the testing environments of the NGI system.

CATEGORIES OF RECORDS IN THE SYSTEM:

- A. Criminal fingerprint images with related biographic, biometric, and criminal justice information;
- B. Civil fingerprint images with related biographic, biometric, and noncriminal justice information;
- C. Fingerprint images with related biographic, biometric, and event information maintained for the purposes of national security (e.g. known or appropriately suspected terrorists);
- D. Fingerprint images with related biographic, biometric, and event information received from federal government agencies pursuant to the FBI's authority to identify and investigate federal crimes and threats to the national security;
- E. Fingerprint images with related biographic, biometric, and event information received from foreign countries or international organizations pursuant to sharing agreements;
- F. Identity History Summary records that contain the criminal justice information associated with criminal fingerprints (i.e. "rap sheets") and/or the noncriminal justice information associated with civil fingerprints;
- G. A name index pertaining to all individuals whose criminal fingerprint images are maintained in the system (i.e. the Interstate Identification Index);
- H. Biometric images (e.g. palm prints, facial images, iris images) maintained for criminal, civil, and/or national security purposes;
- I. Latent fingerprints and palm prints and/or other latent biometric images maintained for criminal and/or national security purposes;

- J. Unknown facial images, iris images, and palm prints and/or other unknown biometric images maintained for criminal and/or national security purposes;
- K. Fingerprint images and/or other biometric images maintained in support of disaster response, humanitarian efforts, or similar purposes;
- L. Fingerprint images with related biographic, biometric, and event information maintained pursuant to an individual's request or consent;
- M. Fingerprint images or biographic and/or supplementary information submitted to request the reason for a firearm transfer denial or delay, appeal/challenge a denial of a firearm transfer, or otherwise inquire about a National Instant Criminal Background Check System transaction;
- N. Fingerprint images with associated biographic and/or supplementary information submitted to obtain identity history record information for access, amendment, or appeal;
- O. Identity records maintained for the purposes of federal employment, contract employment, security clearances, suitability determinations, and background checks;
- P. Identity records maintained pursuant to the FBI's authority to identify and investigate federal crimes and threats to the national security;
- Q. Identity records maintained for the purpose of operating the testing environments of the NGI system.

RECORD SOURCE CATEGORIES:

Federal, state, local, tribal, foreign, and international agencies, and persons who voluntarily submit records for purposes such as firearms appeals, access and amendment, and humanitarian assistance.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b), all or a portion of the records or information contained in this system of records may be disclosed as a routine use pursuant to 5 U.S.C. 552a(b)(3) under the circumstances or for the purposes described below, to the extent such disclosures are compatible with the purposes for which the information was collected:

- A. To local, state, tribal, or federal law enforcement or criminal justice agencies (to include the police, prosecution, penal, probation, parole, and the judiciary) or other authorized federal agencies where such disclosure: (a) May assist the recipient in the performance of its law enforcement, criminal justice, or national security functions, to include the screening of employees or applicants for employment (b) may assist the FBI in performing a law enforcement or national security function (c) may promote, assist, or otherwise serve the mutual efforts of the law enforcement, criminal justice, and national security communities, such as site security screening of visitors to criminal justice facilities and military installations; or (d) may serve a compatible civil law enforcement purpose;
- B. To state or local agencies for the purpose of background investigations of applicants for noncriminal justice employment or licensing purposes, or other entities, if authorized by a federal statute (e.g. The National Child Protection Act of 1993, Volunteers for Children Act, Adam Walsh Child Protection and Safety Act of 2006) or a state statute pursuant to Pub. L. 92 544. Examples include: Those caring for or in contact with vulnerable populations (children, the elderly, the disabled); nursing and home healthcare

professionals; non-profit volunteers; foster/adoptive parents; private security officers; providers of medical services/supplies; employees of federal chartered/insured banking institutions; mortgage loan originators; pari-mutuel wagering/racing licensees; and firearms or explosives permits/licenses;

- C. To authorized police departments of railroads and of private colleges and universities performing the administration of criminal justice;
- D. To officials of tribal agencies for the purpose of Indian childcare, Indian gaming, or pursuant to a Pub. L. 92-544 state statute;
- E. To officials of civil or criminal courts for use in domestic violence or stalking cases;
- F. To noncriminal justice governmental agencies performing criminal justice dispatching functions or data processing/information services for criminal justice agencies;
- G. To private contractors for the purpose of providing services for the administration of criminal justice pursuant to a specific agreement (which must incorporate a Security Addendum approved by the Attorney General of the United States) with a criminal justice agency or a noncriminal justice governmental agency performing criminal justice dispatching functions or data processing/information services for criminal justice agencies;
- H. To private contractors pursuant to specific outsourcing agreements with noncriminal justice agencies to provide noncriminal justice administrative functions such as electronic fingerprint submission and response; tracking missing dispositions; and archival, storage, or destruction of criminal history record information;
- I. To authorized foreign governments or international agencies where such disclosure: (a)
May assist the recipient in the performance of its law enforcement, criminal justice, or

national security functions (b) may assist the FBI in performing a law enforcement or national security function (c) may promote, assist, or otherwise serve the mutual efforts of the international community or (d) may serve a compatible civil law enforcement purpose;

J. To the Department of Defense, Department of State, Department of Transportation, Office of Personnel Management, Central Intelligence Agency, or other statutorily authorized federal agency for the purpose of determining the eligibility of a person for access to classified information or assignment to or retention in sensitive national security positions, the Armed Forces, or positions of public trust or other critical or sensitive positions, or other suitability determinations;

K. To federal agencies for use in background investigations of present and prospective federal employees and contractors;

L. To federal agencies for any official duty required by their agency rules, regulations, Executive Order, or statute;

M. To regulatory agencies authorized by federal statute (e.g. the Securities and Exchange Commission, the Nuclear Regulatory Commission, the Commodity Futures Trading Commission);

N. To the Department of State for the purpose of determining the eligibility of visa applicants;

O. To the Department of Health and Human Services and Department of Agriculture for the purpose of conducting security risk assessments of individuals handling biological agents or toxins;

- P. To the Department of Homeland Security and its components for use in background investigations of individuals with access to secure areas of airports, aircraft, ports, and vessels; commercial drivers of hazardous materials; applicants for aircraft training; those responsible for screening airport passengers and property; those with security functions related to baggage and cargo; and other statutorily authorized populations;
- Q. To the National Center for Missing and Exploited Children when acting within its statutory duty to support law enforcement agencies and to governmental social service agencies when acting within their duties to investigate or respond to reports of child abuse, neglect, or exploitation or other legally mandated duties;
- R. To public housing authorities for the purpose of conducting background checks of applicants for, or tenants of, public housing and to Indian Tribes or Tribally Designated Housing Entities for the purpose of conducting background checks of adult applicants for employment or housing;
- S. To authorized local, state, and federal agencies for the purposes of emergency child placement or emergency disaster response;
- T. To authorized local, state, tribal, federal, foreign, or international agencies for humanitarian purposes;
- U. To a designated point of contact at a criminal justice agency for the purpose of background checks under the National Instant Criminal Background Check System (NICS);
- V. To local, state, or federal law enforcement agencies for the investigation of and issuance of firearms and explosives permits;

- W. To government employees, contractors, grantees, experts, consultant, students, or others for research conducted or training performed in accordance with statutory and regulatory requirements, including parts 22 and 46 of title 28 of the Code of Federal Regulations;
- X. To a former employee of the Department for purposes of: Responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility;
- Y. To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that there has been a breach of the system of records; (2) the Department has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOJ (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.
- Z. To another Federal agency or Federal entity, when the Department determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity

(including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records in this system are stored in paper and/or electronic format.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records in this system are typically retrieved by fingerprints, biometrics, individual name, and other identifying data, including unique identifying numbers assigned by the FBI or other government agencies. Positive identification is effected only by comparison of fingerprint impressions submitted for search against the fingerprints maintained within the system. Another means of retrieval is through name indices, which contain names of the individuals, their birth data, other physical descriptors, and unique identifying numbers, if such have been assigned.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records in this system will be retained and disposed of in accordance with the records schedule approved by the National Archives and Records Administration. In general, fingerprints and associated biometric and biographic information will be destroyed when the subjects attain 110 years of age or 7 years after notification of death with biometric confirmation. Criminal history records and transaction logs are to be permanently retained.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

All records are maintained in a secure government facility with access limited to only authorized personnel or authorized and escorted visitors. Disclosure of information from the system is made only to authorized recipients upon authentication and verification of the right to access the system by such persons and agencies. The physical security and maintenance of information within the system is provided by FBI rules, regulations, and procedures.

RECORD ACCESS PROCEDURES:

All requests for access to records must be in writing and should be addressed to the FBI, Record/Information Dissemination Section, Attn: FOIPA Request, 170 Marcel Drive, Winchester VA 22602-4843. The envelope and letter should be clearly marked "Privacy Act Access Request." The request must describe the records sought in sufficient detail to enable Department personnel to locate them with a reasonable amount of effort. The request must include a general description of the records sought and must include the requester's full name, current address, and date and place of birth. The request must be signed and either notarized or submitted under penalty of perjury. Some information may be exempt from the access provisions as described in the "EXEMPTIONS PROMULGATED FOR THE SYSTEM" paragraph, below. An individual who is the subject of a record in this system of records may access those records that are not exempt from access. A determination whether a record may be accessed will be made at the time a request is received.

Although no specific form is required, you may obtain forms for this purpose from the FOIA/Privacy Act Mail Referral Unit, United States Department of Justice, 950 Pennsylvania Avenue NW, Washington, DC 20530, or on the Department of Justice Web site at <https://www.justice.gov/oip/oip-request.html>.

More information regarding the Department's procedures for accessing records in accordance with the Privacy Act can be found at 28 CFR Part 16 Subpart D, "Protection of Privacy and Access to Individual Records Under the Privacy Act of 1974."

CONTESTING RECORD PROCEDURES:

Individuals seeking to contest or amend records maintained in this system of records must direct their requests to the address indicated in the "RECORD ACCESS PROCEDURES"

paragraph, above. All requests to contest or amend records must be in writing and the envelope and letter should be clearly marked "Privacy Act Amendment Request." All requests must state clearly and concisely what record is being contested, the reasons for contesting it, and the proposed amendment to the record. Some information may be exempt from the amendment provisions as described in the "EXEMPTIONS PROMULGATED FOR THE SYSTEM" paragraph, below. An individual who is the subject of a record in this system of records may contest or amend those records that are not exempt. A determination of whether a record is exempt from the amendment provisions will be made after a request is received.

More information regarding the Department's procedures for amending or contesting records in accordance with the Privacy Act can be found at 28 CFR §16.46, "Requests for Amendment or Correction of Records."

NOTIFICATION PROCEDURES:

Individuals may be notified if a record in this system of records pertains to them when the individuals request information utilizing the same procedures as those identified in the "RECORD ACCESS PROCEDURES" paragraph, above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

The Attorney General has exempted this system from subsections (c)(3) and (4); (d)(1), (2), (3) and (4); (e)(1), (2), (3), (4)(G), (H) and (I), (5) and (8); (f) and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j) and/or (k) subsections. The exemptions will be applied only to the extent that the information in the system is subject to exemption pursuant to 5 U.S.C. 552a(j) and/or (k) subsections. Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c) and (e), and have been published in the Federal Register.

HISTORY:

Next Generation Identification System, 81 Fed. Reg. 27284 (May 5, 2016); 82 Fed. Reg. 24151, 156 (May 25, 2017).

BILLING CODE 4410-02-P

[FR Doc. 2019-21585 Filed: 10/8/2019 8:45 am; Publication Date: 10/9/2019]